Preprints, 4th IFAC Conference on
Advances in Proportional-Integral-Derivative Control
Almería, Spain | June 12-14, 2024

A proportional-integral observer protocol for secure communication

Andreu Cecilia * **Ramon Costa-Castelló** *

* *Universitat Politècnica de Catalunya (UPC), (e-mail: andreu.cecilia@upc.edu, ramon.costa@upc.edu)*

Abstract: In this work, we present a novel observer-based masking protocol in order to secure the communication between nodes of a cyber-physical system. The approach is based on including multiplicative disturbances generated from a known autonomous system in the source node and then including an observer in the receiver node that exactly removes the noise and recovers the original signal. It is shown that, if the masking signal is appropriately designed, the de-masking module can be implemented through a simple proportional-integral observer. The approach is then validated through numerical simulations.

Keywords: Proportional-Integral Observer, Cyber-security, Eavesdropping, Privacy.

1. INTRODUCTION

Cyber-physical systems encompass both physical and cyber components, often utilizing networking to interconnect different system elements. As the prevalence of cyber-physical systems grows, security emerges as a significant objective to be achieved. Indeed, in practice, wireless communication links pose new vulnerabilities, serving as potential entry points for malicious actors seeking to disrupt the system (Teixeira et al., 2015; Pasqualetti et al., 2013).

There exists an extensive literature on cyber-attack detection and mitigation, such as (Pasqualetti et al., 2013; Cecilia et al., 2023; Gallo et al., 2020; Yang et al., 2022, 2021; Cecilia et al., 2021, 2022). Nonetheless, prior to the deployment of any security mechanism, the security of cyber-physical systems should focus on minimizing the potential attack space (Murguia et al., 2020b). Nevertheless, achieving absolute security in system design is impractical from an economical, technological and physical point-of-view. Considering this constraint, it is imperative to acknowledge the presence of potential vulnerabilities in every cyber-physical system. In this context, preventing malicious agents from accessing sensitive data that could expose such vulnerabilities becomes a significant objective. This necessity has induced the development of various security strategies aimed at preserving the privacy of system data communication, as evident in works like (Murguia et al., 2021; Umsonst and Sandberg, 2021; Kawano and Cao, 2020; Kim et al., 2022).

⋆ This research this initiative is carried out within the framework of the EU-funded Recovery, Transformation and Resilience Plan (Next Generation) thorugh the project ACROBA and the Spanish Ministry of Universities funded by the European Union - NextGenerationEU (2022UPC-MSC-93823). This work is part of the Project MAFALDA (PID2021-126001OB-C31) funded by MCIN/ AEI /10.13039/501100011033 and by "ERDF A way of making Europe". This work is part of the project MASHED (TED2021-129927B-I00), funded by MCIN/ AEI/10.13039/501100011033 and by the European Union Next GenerationEU/PRTR.

In this work, we propose a novel framework for secure communication. The framework is based on masking the communication signal by means of an autonomous nonlinear system in the source node. Then, de-masking the signal through an observer-based de-masking module. The overall framework is based on recent theory on cancelling output disturbances in observer design (Cecilia et al., 2024). We highlight that, while the framework is very flexible in nature, it is shown that if the masking signal is appropriately designed, the de-masking module can be implemented through a simple proportional-integral observer (PI-observer).

The remainder of the paper is organized as follows. The communication topology, objectives and the problem being considered are formulated in Section 2. In Section 3, we present the main observer-based masking protocol. In Section 4 we show how the proposed protocol can be implemented through a simple PI-observer. The protocol is validated through a numerical simulation in Section 5. Finally, some conclusions are drawn in Section 6.

2. FRAMEWORK

2.1 Communication topology and objective

Before formulating the main problem being solved in this paper, we provide the following explanation on terminologies.

- **Source node:** The node that transmits information through the communication layer.
- **Receiver node:** The legal node designed to receive the information from the communication layer.
- **Eavesdropper**: Unwanted third party node that listens the information transmitted through the channel between the source and the receiver.
- **Masking:** Process that transforms the transmitted information into an unreadable version for eavesdroppers or any unwanted third-party agents.

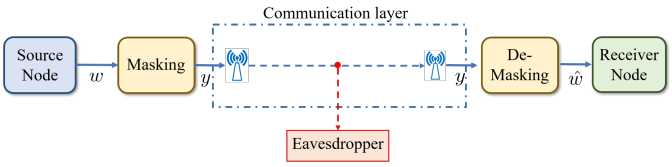

Fig. 1. Scheme of the communication topology.

- **De-masking:** Process that removes the masking from the transmitted signal in order to recover readability of the information.
- **Communication layer:** Transmission medium between the source node and the receiver node. Signals transmitted trough the channel will be distorted by some additive sensor noise.

Leveraging on the above definitions, we can now state the scenario considered in this work. Precisely, we consider the case where a source node wants to communicate a signal modelled here as a m-dimensional constant vector $w \in \mathbb{R}^m$. The vector w is communicated to the receiver node through the communication layer. The communication layer will add some unknown multiplicative disturbances to the transmitted signal w. Then, we consider that an eavesdropper also listens the information transmitted through the channel and is trying to infer the value of w.

The objective is to secure the communication between the source node and the receiver node. In this work, we assume that the eavesdropper has already accessed the communication layer and is already listening to the information being sent between the nodes.

2.2 Security Architecture

In order to avoid the privacy disruption of the vector w, the signal is processed through a masking protocol and transformed to a new signal y, which is the one actually being transmitted through the communication channel. The masking protocol has to be designed in a way that even if an eavesdropper listens to the signal y, it cannot infer the value of the vector w. In parallel, a de-masking protocol is implemented in the receiver node in order to reconstruct the signal, denoted here as $\hat{w}$, from the transmitted signal y. A scheme of the communication topology has been included in Fig. 1.

We highlight here that, different from other masking protocols, e.g. (Murguia et al., 2020a), the signal y is the only information being communicated between the source and receiver nodes. Additionally, we will consider that if the masking and de-masking modules have some time-varying behaviour, they may initially lack synchronization. This synchronization and communication constraints drastically simplifies the cost and deployment complexity of the protocol, since they avoid the need of adding additional communication channels between nodes or requiring an initialization protocol before communication.

The following sections are dedicated to presenting the proposed observer-based masking protocol.

3. PROPOSAL

3.1 Masking generator

The masking generator is implemented at the source node. In order to mask the signal between the source node and the receiver node, this work proposes multiplying the transmitted value $w \in \mathbb{R}^m$ by a time-varying signal $d \in \mathbb{R}^m$ generated from an autonomous system of the form

$$\begin{aligned} \dot{x} &= f(x) \\ d &= h(x) + b, \end{aligned} \tag{1}$$

where $x \in \mathbb{R}^n$ is the state of the masking generator, $f(\cdot) : \mathbb{R}^n \to \mathbb{R}^n$ and $h(\cdot) : \mathbb{R}^n \to \mathbb{R}$ are sufficiently smooth functions and $b \in \mathbb{R}$ is a constant parameter to be fixed.

Precisely, we assume that the source node sends the following signal though the communication layer

$$y = d\ w = \text{diag}((h(x) + b))w. \tag{2}$$

In other words, we are encoding each individual element of the vector $w = [w_1, \dots, w_m]^\top$ with the masking signal $(h(x) + b)$, thus, we are transmitting a set of signals $y = [y_1, \dots, y_m]^\top$ of the form

$$y_i = ((h(x) + b))w_i, \quad \forall i \in \{1, \dots, m\}.$$

For the rest of the document, we will assume the following on the masking generator (1).

Assumption 1. *The state of the masking generator evolves in a compact and forward invariant set $\mathcal{X} \subsetneq \mathbb{R}^n$. The state of the masking generator is always initialized in $\mathcal{X}$.*

Assumption 1 guarantees that both the state, x, and the masking signal, d, are bounded. This is a perfectly reasonable constraint, otherwise, the masking signal cannot be implemented in practice. Additionally, we impose an observability condition on the masking generator.

Assumption 2. *The system (1) is instantaneously observable. That is, for any pair of solutions $(x_a(t), x_b(t))$ of (1) initialized at $\mathcal{X}$ and for all $t_d \in [0, \infty]$ such that*

$$h(x_a(t)) = h(x_b(t)), \quad \forall 0 \leq t < t_d,$$

we have

$$x_a(t) = x_b(t).$$

Considering masking generators that satisfy a minimal observability property is also a reasonable assumption in practice, otherwise, there would be some states in x that do not have an effect of the masking signal d and can be discarded. In this work, we restrict ourselves to instantaneous observability in order to simplify the de-masking module design.

3.2 Observer as a de-masking module

The de-masking process takes place at the receiver node. We assume that the receiver node has information of the functions $f(\cdot), h(\cdot)$ and the constant b from the masking generator (1). Nonetheless, we do not assume that the masking and de-masking modules are synchronized. Consequently, we assume that the state x of the masking generator (1) is unknown for the de-masking module.

Notice that in this case, the transmitted signal can be modelled as the following autonomous system

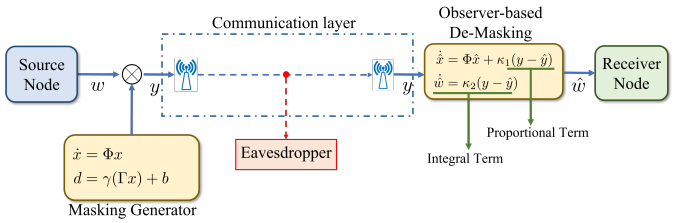

Fig. 2. Scheme of the proposed observer-based masking protocol.

$$\begin{aligned} \dot{x} &= f(x) \\ \dot{w}_i &= 0 \\ y_i &= ((h(x)+b))w_i, \quad \forall i \in \{1,\dots,m\}. \end{aligned} \tag{3}$$

In this work, we propose to use an observer as a de-masking module. That is, to design a system that generates an estimation of x and w, denoted here as $\hat{x}$ and $\hat{w}$, from the measured signal y and the knowledge of the extended system (3). An intuitive scheme of the proposed observer-based masking protocol is depicted in Fig. 2.

Naturally, the possibility of designing such an observer and the effectiveness of the de-masking module depends on the observability and structure of the extended system (3). In the following section, we will show that if the functions $f(x)$ and $h(x)$ are properly selected, the observer design process boils down to a simple PI-observer.

4. PI-OBSERVER APPROACH FOR DE-MASKING

4.1 Masking signal

In particular, suppose that the masking signal $d(t)$ is the sum of N signals w_i, that is

$$d(t) = \sum_{i=1}^{N} w_i(t), \qquad w_i(t+T_i) = w_i(t), \quad \forall t \geq 0.$$

That is, the masking signal is composed by a sum of N signals in which each w_i is T_i-periodic. We can suppose that the periods T_i are incommensurable reals, namely $\frac{T_i}{T_j}$ is an irrational number for any pair of i, j, thus generating a quasi-periodic signal.

More precisely, we consider that f, h in the masking generator (1) are selected as

$$f(x) := \Phi x, \quad h(x) := \gamma(\Gamma^\top x) + b \tag{4}$$

with $b \in \mathbb{R}$ being a constant parameter to tune and Φ, Γ and a (at least C^1) function $\gamma(\cdot) : \mathbb{R} \to \mathbb{R}$ satisfying the following assumption.

Assumption 3. *The matrix Φ is skew-symmetric and non-singular, the pair (Φ, Γ) is observable and γ is monotonic, namely it satisfies*

$$(a-b)^\top[\gamma(a) - \gamma(b)] \geq (a-b)^\top(a-b)$$

for all $a, b \in \mathbb{R}$, $a \neq b$.

A possible choice of Φ, Γ to satisfy Assumption 3 is simply given by

$$\begin{aligned} \Phi &= \text{blckdiag}(\Phi_1, \dots, \Phi_{n/2}), & \Phi_i &= \begin{pmatrix} 0 & \eta_i \\ -\eta_i & 0 \end{pmatrix}, \\ \Gamma &= \begin{bmatrix} \Gamma_1 & \dots & \Gamma_{n/2} \end{bmatrix}, & \Gamma_i &= (1 \ 0), \end{aligned} \tag{5}$$

where n is selected to be an even number, $\eta_i > 0$ for all $i \in \{1, \dots, n/2\}$, correspond to the desired frequencies of the signal d. The function γ can be selected as any monotonic function. A particularly interesting choice is to select it as a transcendental function, thus, generating a disturbance d that contains an infinite number of harmonics.

We highlight that this particular selection of the masking generator dynamics satisfies Assumption 1 and Assumption 2, since the pair (Φ, Γ) staisfies the observability rank condition.

4.2 PI-Observer

With this particular selection of the masking generator, the extended system (3) takes the following form

$$\begin{aligned} \dot{x} &= \Phi x \\ \dot{w}_i &= 0 \\ y_i &= (\gamma(\Gamma^\top x) + b)w_i, \quad \forall i \in \{1,\dots,m\} \end{aligned} \tag{6}$$

where the functions Φ, γ and the matrix Γ, b are known and defined in Section 4.1. We recall that the main objective is to estimate the states x, w from the measured signal y. The main idea of this section is that such an estimation task can be easily achieved through an observer with a proportional term designed considering the x-dynamics and an integral term for the w-dynamics, resulting in a simple PI-observer. To do so, we first impose the following positivity assumption on each transmitted signal y_i,

Assumption 4. *For all $i \in \{1, \dots, m\}$ and all $t \geq 0$ we have $y_i > 0$ and $w_i > 0$.*

Remark 1. *Positivity of the term $(\gamma(\Gamma^\top x)+b)$ can always be guaranteed by selecting $b > 0$ large enough.*

Under Assumption 4, we can separate the masking elements from the elements of the message w through a natural logarithm operation. That is, we will consider a new measured signal denoted as $\bar{y}_i$ defined for all $i \in \{1, \dots, m\}$ as follows

$$\bar{y}_i := \ln(y_i) = \ln(\gamma(\Gamma^\top x) + b) + \ln(w_i). \tag{7}$$

Thus, the observer will be designed considering this new signal $\bar{y}_i$.

Remark 2. *Since we are restricting ourselves to positive signals y_i, the logarithm is always well-defined.*

Remark 3. *The natural logarithm operation is computed at the receiver node. Consequently, y is still the signal transmitted through the channel.*

Precisely, the PI-observer de-masking module takes the following form for all $i \in \{1, \dots, m\}$

$$\begin{aligned} \dot{\hat{x}} &= \Phi\hat{x} + \Gamma z_i \\ \dot{\hat{w}}_i &= z_i \\ z_i &= \bar{y}_i - \ln(\gamma(\Gamma^\top \hat{x}) + b) - \ln(\hat{w}_i)\,. \end{aligned} \tag{8}$$

We highlight now the structure of the de-masking observer. Note that z_i is just the measured error, that is, the error between the signal $\bar{y}_i$ (defined in (7)) and the observer estimation of the same signal. Then, the $\hat{x}$ dynamics are just a copy of the masking generator dynamics (1) plus a proportional term on the measured error. The $\hat{w}_i$ dynamics are just an integral of the measured error. This combination of a proportional term and a integral term is what gives the name of PI-observer, as highlighted in Fig. 2.

The stability and convergence of the proposed observer is given in the next theorem.

Theorem 1. *Consider the extended dynamics* (6) *and the PI-observer* (8)*. If Assumption 3 and Assumption 4 are satisfied, then, asymptotic estimation of the vector w_i is achieved. That is, for all $i \in \{1, \dots, m\}$,*

$$\lim_{t\to\infty} |w_i - \hat{w}_i(t)| = 0 \tag{9}$$

for all $x(0), \hat{x}(0) \in \mathcal{X}$ and any $w_i \in \mathbb{R}$.

Proof. For any $i \in \{1, \dots, m\}$, the complete system formed by the masking generator (1) and the PI-observer (8) can be written as

$$\begin{aligned} \dot{x} &= \Phi x, & \dot{\hat{x}} &= \Phi\hat{x} + \Gamma z_i, \\ \dot{w}_i &= 0, & \dot{\hat{w}}_i &= z_i, \\ \bar{y}_i &= \ln(y_i), & z_i &= \bar{y}_i - \ln(\gamma(\Gamma^\top\hat{x}) + b) - \ln(\hat{w}_i). \end{aligned} \tag{10}$$

Now, define the error signals $\tilde{x} = x - \hat{x}$ and $\tilde{w}_i = w_i - \hat{w}_i$. Then, the error dynamics evolve according to

$$\begin{aligned} \dot{\tilde{x}} &= \Phi\tilde{x} - \Gamma z_i, \\ \dot{\tilde{w}}_i &= -z_i. \end{aligned} \tag{11}$$

From the positivity Assumption 4, the natural logarithm is well-defined and satisfies a monotonic condition, that is,

$$(w_i - \hat{w}_i)^\top[\ln(w_i) - \ln(\hat{w}_i)] \geq c_{1,i}(w_i - \hat{w}_i)^2 \tag{12}$$

for all $w_i, \hat{w}_i > 0$, $w_i \neq \hat{w}_i$ and some positive constant $c_{1,i} > 0$. Similarly, since the natural logarithm is monotonic and the function γ is also monotonic by means of Assumption 3, the composition of both functions is also monotonic. That is, the following holds,

$$\begin{aligned} &(x - \hat{x})^\top\Gamma[\ln(\gamma(\Gamma^\top x) + b) - \ln(\gamma(\Gamma^\top\hat{x}) + b)] \\ &\quad \geq c_{2,i}(x - \hat{x})^\top\Gamma\Gamma^\top(x - \hat{x}), \end{aligned} \tag{13}$$

for all $x, \hat{x}$ such that $\Gamma x \neq \Gamma\hat{x}$ and $\gamma(\Gamma^\top x) + b, \gamma(\Gamma^\top\hat{x}) + b > 0$ and some positive constant $c_{2,i} > 0$. To simplify the notation of the next developments, we will assume without loss of generality that $c_{1,i} = c_{2,i} = 1$.

Now, consider the Lyapunov function, V, defined as

$$V := V_x + V_d, \quad V_x := \frac{1}{2}\tilde{x}^\top\tilde{x}, \quad V_d := \frac{1}{2}\tilde{w}_i^\top\tilde{w}_i.$$

The derivative of the factor V_x reads as

$$\dot{V}_x = \frac{1}{2}\tilde{x}^\top(\Phi^\top + \Phi)\tilde{x} - \tilde{x}^\top\Gamma z_i \leq -2\tilde{x}^\top\Gamma z_i, \tag{14}$$

where the second inequality comes from the skew-symmetric property of Φ, see Assumption 3, which guarantees that $\Phi^\top + \Phi \leq 0$. Similarly, the derivative of V_d satisfies

$$\dot{V}_d = -\tilde{w}_i^\top z_i. \tag{15}$$

Combining (14) and (15) and considering the monotonic inequalities (12) and (13) we obtain

$$\begin{aligned} \dot{V} &\leq -\tilde{x}^\top\Gamma z_i - \tilde{w}_i^\top z_i = -(\Gamma^\top\tilde{x} + \tilde{w}_i)^\top z_i \\ &= -(\Gamma^\top\tilde{x} + \tilde{w}_i)^\top[\ln(\gamma(\Gamma^\top x) + b) - \ln(\gamma(\Gamma^\top\hat{x}) + b) \\ &\qquad + \ln(w_i) - \ln(\hat{w}_i)] \\ &\leq -(\Gamma^\top\tilde{x} + \tilde{w}_i)^\top(\Gamma^\top\tilde{x} + \tilde{w}_i). \end{aligned}$$

Consequently, the error dynamics (11) converge to the largest invariance set of $\Omega := \{\tilde{x} \in \mathbb{R}^n, \tilde{w}_i \in \mathbb{R} \mid \Gamma^\top\tilde{x} + \tilde{w}_i = 0\}$. Notice that, similar to the problem considered in (Cecilia et al., 2023, 2024), from detectability properties of the system, for all $(\tilde{x}, \tilde{w}_i) \in \Omega$ we have that $\lim_{t\to\infty} |\tilde{w}_i| = \lim_{t\to\infty} |\tilde{x}| = 0$. Thus, the result follows from the LaSalle invariance principle. □

In summary, Theorem 1 establishes that if the masking generator is designed as in (4), then, the simple PI-observer de-masking module in (8) asymptotically removes the mask and recovers the message d. We highlight that the PI-observer is designed directly with the parameters of the masking generator, that is, there are no additional parameters of the observer to be tuned. Consequently, the implementation of the proposed scheme simply boils down to selecting Φ, Γ and the function $\gamma(\cdot)$ according to the practical constraints of the application being considered.

5. NUMERICAL SIMULATION

In this section, we analyze the viability of the approach through a numerical simulation. In this simulation, we consider the scenario where we want to transmit the following 6-dimensional vector between the source node and the receiver node

$$w = [2\ 5\ 1\ 12\ 2.5\ 10]\,.$$

In order to secure the communication, in the source node, we are going to mask each element of the vector d by means of the signal generated by the masking generator (4) with $\omega_1 = 20, \omega_2 = 10\sqrt{\omega_1}, b = 3$, the vector Γ fixed as in (5) and $\gamma(s) = 3\text{atan}(s + 5)$. Notice that the atan$(\cdot)$ function is monotonic, that is, it satisfies Assumption 3. The initial conditions of the masking generator are fixed to $x = [1\ 0\ 1\ 0]^\top$. Naturally, additional frequencies could be added in the matrix Φ and the complexity of the function $\gamma(\cdot)$ could be increased in order to improve the security of the protocol. Nonetheless, the proposed masking signal is a simple enough example in order to validate and understand the benefits of the approach.

In this simulation, we assume that the communication layer adds some (additive) white noise to the transmitted signal with a variance of 0.1. In order to visualize the effect of the masking signal and noise, a comparison between the true value $w_1 = 2$ (the first element of the vector w) and the transmitted signal y_1 is depicted in Fig. 3. It is noticeable that there is a significant bias between the true signal w_1 and the transmitted signal. This bias is induced by the constant b and the constant 5 inside the function $\gamma(\cdot)$. We highlight that the bias b and the constant 5 have the same frequency as the signal w_1, thus, from an observability point-of-view, an eavesdropper cannot distinguish between the bias and the true signal if it doesn't know the function $\gamma(\cdot)$ and the constant b. Thus, an eavesdropper cannot reconstruct the signal w_1 and we guarantee the security of the communication.

In parallel to the bias, we can see that the transmitted signal presents some oscillations. These oscillations are generated by the additive noise of the channel and the term $\Gamma^\top x$ of the masking generator. We highlight that the peak-to-peak amplitude of the noise is actually larger than the amplitude of the oscillations generated by the masking signal. That is, the noise levels are significantly large relative to the dynamics of the masking generator. This is an important detail of the simulation, since a badly designed observer for the extended dynamic (6) can amplify the noise and make the estimation $\hat{w}_i$ practically unusable. Some notable examples of this behaviour would be present in more common nonlinear observer as the

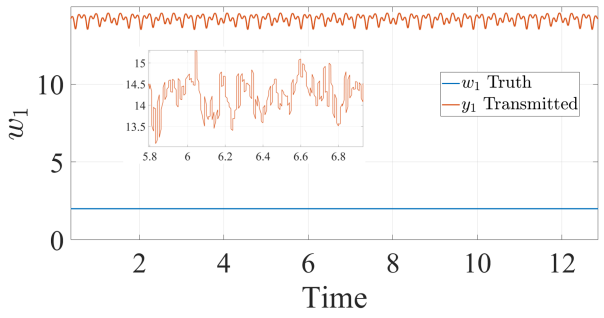

Fig. 3. Comparison between the true value w_1 and the transmitted signal y_1

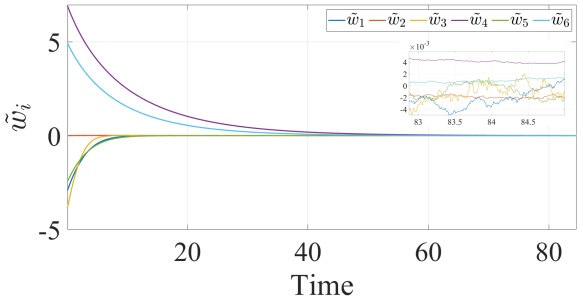

Fig. 4. Evolution of the reconstruction errors $\tilde{w}_i$ at the receiver node.

high-gain observer (Gauthier et al., 1992) or the sliding-mode observer (Shtessel et al., 2014). Nonetheless, as it will be shown below, the proposed PI-observer does not only present a simple structure and trivial design, but is not significantly affected by the noise in the channel.

Indeed, the reconstruction errors, $\tilde{w}_i = w_i - \hat{w}_i$, of all the PI-observer de-masking modules are depicted in Figure 4. It is noticeable that even in the presence of significant noise, the PI-observer is capable of reconstructing the signal with a relative error below the 0.1%. Which validates the viability and performance of the proposed scheme.

6. CONCLUSIONS

This work has presented an observer-based masking protocol to secure the communication of constant signals between nodes. It has been shown that if the masking signal is appropriately selected, the de-masking module can be implemented as a simple PI-observer with no parameters to be tuned. A numerical validation has validated the simplicity and efficacy of the proposed scheme. Future works will extend this initial idea to secure time-varying signals, secure dynamic controllers and multi-agent systems.

REFERENCES

Cecilia, A., Astolfi, D., Bin, M., and Costa-Castelló, R. (2024). Canceling output disturbances in observer design through internal model filters. *Automatica*, 162, 111529.

Cecilia, A., Astolfi, D., Casadei, G., Costa-Castelló, R., and Nešić, D. (2023). A masking protocol for private communication and attack detection in nonlinear observers. In *62nd IEEE Conference on Decision and Control (CDC)*, 7495–7500.

Cecilia, A., Sahoo, S., Dragičević, T., Costa-Castelló, R., and Blaabjerg, F. (2021). Detection and mitigation of false data in cooperative dc microgrids with unknown constant power loads. *IEEE Transactions on Power Electronics*, 36(8), 9565–9577.

Cecilia, A., Sahoo, S., Dragičević, T., Costa-Castelló, R., and Blaabjerg, F. (2022). On addressing the security and stability issues due to false data injection attacks in dc microgrids—an adaptive observer approach. *IEEE Transactions on Power Electronics*, 37(3), 2801–2814.

Gallo, A.J., Turan, M.S., Boem, F., Parisini, T., and Ferrari-Trecate, G. (2020). A distributed cyber-attack detection scheme with application to dc microgrids. *IEEE Transactions on Automatic Control*, 65(9), 3800–3815.

Gauthier, J., Hammouri, H., and Othman, S. (1992). A simple observer for nonlinear systems applications to bioreactors. *IEEE Transactions on Automatic Control*, 37(6), 875–880.

Kawano, Y. and Cao, M. (2020). Design of privacy-preserving dynamic controllers. *IEEE Transactions on Automatic Control*, 65(9), 3863–3878.

Kim, J., Kim, D., Song, Y., Shim, H., Sandberg, H., and Johansson, K.H. (2022). Comparison of encrypted control approaches and tutorial on dynamic systems using learning with errors-based homomorphic encryption. *Annual Reviews in Control*, 54, 200–218.

Murguia, C., Shames, I., Farokhi, F., and Nešić, D. (2020a). Information-theoretic privacy through chaos synchronization and optimal additive noise. *Privacy in Dynamical Systems*, 103–129.

Murguia, C., Shames, I., Farokhi, F., Nešić, D., and Poor, H.V. (2021). On privacy of dynamical systems: An optimal probabilistic mapping approach. *IEEE Transactions on Information Forensics and Security*, 16, 2608–2620.

Murguia, C., Shames, I., Ruths, J., and Nešić, D. (2020b). Security metrics and synthesis of secure control systems. *Automatica*, 115, 108757.

Pasqualetti, F., Dörfler, F., and Bullo, F. (2013). Attack detection and identification in cyber-physical systems. *IEEE Transactions on Automatic Control*, 58(11), 2715–2729.

Shtessel, Y., Edwards, C., Fridman, L., Levant, A., et al. (2014). *Sliding mode control and observation*, volume 10. Springer.

Teixeira, A., Shames, I., Sandberg, H., and Johansson, K.H. (2015). A secure control framework for resource-limited adversaries. *Automatica*, 51, 135–148.

Umsonst, D. and Sandberg, H. (2021). On the confidentiality of controller states under sensor attacks. *Automatica*, 123, 109329.

Yang, T., Murguia, C., Kuijper, M., and Nešić, D. (2021). An unknown input multi-observer approach for estimation and control under adversarial attacks. *IEEE Transactions on Control of Network Systems*, 8(1), 475–486.

Yang, T., Murguia, C., Lv, C., Nešić, D., and Huang, C. (2022). On joint reconstruction of state and input-output injection attacks for nonlinear systems. *IEEE Control Systems Letters*, 6, 554–559.